COMPLETE SET OF CLAIMS

1. (Currently Amended) An authentication communication system which includes (a) a storage medium having an area for storing digital information and (b) an access device for reading/writing digital information from/into the area, the authentication communication system comprising:

a first authentication phase in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol ~~by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium~~ using the scrambled access information;

a second authentication phase in which the storage medium authenticates whether the access device is authorized; and

a transfer phase in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information.

2. (Original) The authentication communication system of Claim 1,

wherein in the first authentication phase,

the access device includes:

an access information acquisition unit for acquiring the access information which shows the area;

a random number acquisition unit for acquiring a random number;

a generation unit for generating random number access information by combining the access information and the random number; and

an encryption unit for encrypting the random number access information according to an encryption algorithm, to generate the scrambled access information,

the storage medium includes a response value generation unit for generating a response value from the scrambled access information, and

the access device includes an authentication unit for authenticating whether the storage medium is authorized using the response value.

3. (Original) The authentication communication system of Claim 2,

wherein in the transfer phase, the storage medium includes:

a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain the random number access information; and

a separation unit for separating the access information from the random number access information.

4. (Original) The authentication communication system of Claim 3,

wherein in the first authentication phase,

the access device further includes a random number seed storage unit for storing a random number seed, and

the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit.

5. (Original) The authentication communication system of Claim 4,

wherein in the first authentication phase, the access device further writes the scrambled access information over the random number seed stored in the random number seed storage unit, as a new random number seed.

6. (Original) The authentication communication system of Claim 3,

wherein in the first authentication phase,

the access device further includes a random number seed storage unit for storing a random number seed, and

the random number acquisition unit acquires the random number, by reading the random number seed from the random number seed storage unit and generating the random number based on the random number seed.

7. (Original) The authentication communication system of Claim 6,

wherein in the first authentication phase, the access device further writes the random number over the random number seed stored in the random number seed storage unit as a new random number seed.

8. (Original) The authentication communication system of Claim 3,

wherein in the transfer phase,

the storage medium, which stores digital information in the area, includes an encryption unit for reading the digital information from the area shown by the access information and encrypting the digital information according to an encryption algorithm to generate encrypted digital information, and

the access device, which reads the digital information from the area, includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm.

9. (Original) The authentication communication system of Claim 3,

wherein in the transfer phase,

the access device, which writes digital information into the area, includes:

a digital information acquisition unit for acquiring the digital information; and

an encryption unit for encrypting the digital information according to an encryption algorithm to generate encrypted digital information, and

the storage medium includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, and writing the digital information into the area shown by the access information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm.

10. (Original) The authentication communication system of Claim 3,

wherein in the transfer phase,

the access device, which writes digital information into the area, includes:

a digital information acquisition unit for acquiring the digital information;

a content key acquisition unit for acquiring a content key;

a first encryption unit for encrypting the acquired content key according to a first encryption algorithm to generate an encrypted content key;

a second encryption unit for encrypting the encrypted content key according to a second encryption algorithm to generate a double-encrypted content key; and

a third encryption unit for encrypting the digital information according to a second encryption algorithm using the content key, to generate encrypted digital information,

the storage medium includes a decryption unit for decrypting the double-encrypted content key according to a first decryption algorithm to obtain the encrypted content key, and writing the encrypted content key into the area shown by the access information, and

the storage medium further includes an area for storing the encrypted digital information.

11. (Currently Amended) An authentication communication method used in an authentication communication system which includes (a) a storage medium having an area for storing digital information and (b) an access device for reading/writing digital information from/into the area, the authentication communication method comprising:

a first authentication step in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol ~~by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium~~ using the scrambled access information;

a second authentication step in which the storage medium authenticates whether the access device is authorized; and

a transfer step in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access

.information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information.

12. (Currently Amended) A computer-readable storage medium which stores an authentication communication program for use in an authentication communication system (a) which includes a storage medium having an area for storing digital information and an access device for reading/writing digital information from/into the area, and (b) in which the digital information is transferred after each of the storage medium and the access device authenticates each other as authorized devices, the authentication communication program comprising:

a first authentication step in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol ~~by transmitting scrambled access information generated by scrambling access information which shows the area, to the storage medium~~ using the scrambled access information;

a second authentication step in which the storage medium authenticates whether the access device is authorized; and

a transfer step in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the access information.

13-16. (Cancelled)

17. (New) An access device for reading/writing digital information from/into an area in a storage medium, comprising:

authentication means for transmitting to the storage medium scrambled access information generated by scrambling access information which shows the area, and authenticating whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information;

proving means for proving to the storage medium that performs authentication of the access device that whether the access device is authorized; and

access means for reading and writing digital information from and to the area shown by the access information, which is extracted by the storage medium from the scrambled access information that was used in the authentication protocol, when the storage medium and the access device have authenticated each other as authorized devices.

18. (New) The access device of Claim 17,

wherein the authentication means includes:

an access information acquisition unit for acquiring the access information which shows the area;

a random number acquisition unit for acquiring a random number;

a generation unit for generating random number access information by combining the access information and the random number;

an encryption unit for encrypting the random number access information according to an encryption algorithm, to generate the scrambled access information; and

a transmission unit for transmitting the scrambled access information to the storage medium,

the storage medium generates a response value from the scrambled access information, and transmits the response value to the access device, and

the authentication means further includes:

a reception unit for receiving the response value from the storage medium, and

an authentication unit for authentication whether the storage medium is authorized, using the response value.

19. (New) A storage medium having an area for storing digital information wherein an access device reads/writes digital information from/into the area, comprising:

proving means for receiving scrambled access information, generated by scrambling access information that shows the area, from the access device and

proving whether the storage medium is authorized to the access device that performs authentication of the storage medium according to a challenge-response authentication protocol using the scrambled access information;

authentication means for authenticating whether the access device is authorized; and

extraction means for extracting the access information from the scrambled access information received by the reception means when the storage medium and the access device have authenticated each other as authorized devices;

wherein the access device reads/writes digital information from/into the area shown by the access information extracted by the extraction means.

20. (New) The storage medium of Claim 19,

wherein the extraction means includes:

a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain random number access information; and

a separation unit for separating the access information from the random number access information.